AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) A method comprising:

in a server, hosting an intrusion detection process that provides intrusion detection services; ~~and~~

integrating the intrusion detection process with a server process; and

passing a request for data received by the server process to the intrusion detection process,

where the intrusion detection process comprises:

packing a subset of information from the request into an analysis format; and

delivering the subset in a funneling process, via a socket, to an analysis process.

2. (Original) The method of claim 1 in which integrating comprises:

defining global application programmer interface (API) structures in the intrusion detection process to establish a connection to an application programmer interface (API) of the server process.

3. – 4. (Cancelled)

5. (Currently Amended) The method of claim [[4]] 1 further comprising analyzing the subset In the analysis process.

6. (Original) The method of claim 1 in which the server Is a web server.

7. (Cancelled)

8. (Currently Amended) The method of claim [[4]] 1 in which the analysis process is resident in the ~~web~~ server.

9. (Currently Amended) The method of claim [[4]] 1 in which the analysis process is resident outside of the ~~web~~ server.

10. (Cancelled)

11. (Currently Amended) The method of claim ~~10~~ 1 in which the funneling process comprises:

accepting incoming connections to which the subset can be ~~trancmitting~~ transmitted; and

passing the subset to outgoing connections.

12. (Currently Amended) A method comprising:

~~passing~~ conveying a request for data received by a ~~first~~ web server process executing in a first server to a detection process that includes:

packing a subset of ~~the data~~ information from the request into an analysis format; and

passing the subset to an analysis process, where passing comprises:

receiving the subset in a piped logs interface of the web server; and

delivering the subset to a funneling process via a socket.

13. (Original) The method of claim 12 also including analyzing the subset in the analysis process.

14. - 15. (Cancelled)

16. (Original) The method of claim 12 in which the detection process is resident in the first server.

17. (Original) The method of claim 13 in which the analysis process is resident in the first server.

18 (Original) The method of claim 13 in which the analysis process is resident in a second server.

19.– 22. (Cancelled)

23. (Currently Amended) The method of claim [[22]] 12 in which the funneling process comprises:

accepting incoming connections to which the subset can be transmitted; and

passing the subset to outgoing connections.

24 (Currently Amended) The method of claim [[22]] 12 in which the funneling process further comprises duplicating the subset for delivery to a second analysis process.

25. – 34. (Cancelled)

35. (New) The method of claim 1 in which the funneling process further comprises duplicating the subset for delivery to a second analysis process.

36. (New) A computer program product residing on a computer readable medium having instructions stored thereon which, when executed by a processor, cause the processor to:

host, in a server, an intrusion detection process that provides intrusion detection services;

integrate the intrusion detection process with a server process; and

pass a request for data received by the server process to the intrusion detection process,

where the intrusion detection process comprises:

packing a subset of information from the request into an analysis format; and

delivering the subset in a funneling process, via a socket, to an analysis process.

37. (New) A computer program product residing on a computer readable medium having instructions stored thereon which, when executed by a processor, cause the processor to:

convey a request for data received by a web server process executing in a first server to a detection process that includes:

pack a subset of information from the request into an analysis format; and

pass the subset to an analysis process, where passing comprises:

receiving the subset in a piped logs interface of the web server; and

delivering the subset to a funneling process via a socket.

38. (New) A method for detecting misuse of an application server process that is hosted at a server in a network, the method comprising:

receiving, from the application server process, a forwarded request for data;

packing a subset of information from the request into an analysis format; and

delivering the subset in a funneling process, via a socket, to an analysis process.

39. (New) The method of claim 38, wherein the application server process is a web server process.

40. (New) The method of claim 38, wherein the analysis process is resident outside of the server.

41. (New) The method of claim 38, further comprising analyzing the subset in the analysis process.